REMARKS/ARGUMENTS

I. Introductory Remarks

In the Office Action of April 27, 2007, the Patent Office examined claims 118-162, original claims 1-117 having been previously cancelled. In the Office Action, the Patent Office raised a 35 USC §112, second paragraph, objection to independent claims 118 and 140. In addition, the Patent Office rejected (i) pending claims 118, 119, 121, 125-128, 135-138, 140-142, 144, 147, 152, 159-162 under 35 USC § 103, as being obvious over *Doi*, U.S. Pat. No. 6,742,118, in view of *Cunningham*, U.S. Pat. No. 6,219,786; (ii) pending claims 120, 122-124, 145, 146, 148-151 under 35 USC § 103, as being obvious over *Doi*, U.S. Pat. No. 6,742,118, in view of *Cunningham*, U.S. Pat. No. 6,219,786 in view of *Hayes* U.S. Publ. No. 2004/0215771; and (iii) pending claims 129-134, 153-158 under 35 USC § 103, as being obvious over *Doi*, U.S. Pat. No. 6,742,118, in view of *Cunningham*, U.S. Pat. No. 6,219,786 in view of *Edgett*, U.S. Pat. No. 5,796,942.

Rejected claims 118-162 are hereby cancelled, rendering the substance of the rejections and objection raised in the Office Action as moot. Applicant hereby presents new claims 163-191, rather than amending claims 118-162, to make it easier for the Examiner to read and review such claims. However, in order to expedite continued examination of the present case and, hopefully, to bring this case to final resolution, Applicant includes a substantive response and arguments explaining why the newly presented claims 163-191 define over and are not obviated by the art of record.

In view of the new claims presented, the art of record, and the following remarks, allowance of the present Application and presently pending claims are respectfully requested.

II. Record of Telephonic Interview

Applicants, through the attorney of record and identified below, thank Examiner Christopher J. Brown for granting and participating in a telephonic interview on September 19, 2007.

Pursuant to 37 C.F.R. § 1.133(b), the following is submitted as a complete written statement of the claim(s) and arguments presented during the interviews as warranting favorable action. The following statement is intended to comply with the requirements of MPEP § 713.04 and expressly sets forth: (A) a brief description of the nature of any exhibit shown or any demonstration conducted; (B) identification of the claims discussed; (C) identification of specific prior art discussed; (D) identification of the principal proposed amendments of a substantive nature discussed; (E) the general thrust of the principal arguments; (F) a general indication of any other pertinent matters; and (G) the general results or outcome of the interview, if appropriate.

On September 19, 2007, the undersigned presented new claim 163 and explained how and why such claim was not anticipated by or rendered obvious by the references of record raised and discussed in the present and prior Office Actions in the present case. The examiner requested further time to review the language and elements of the new claim and requested the opportunity to review the written arguments presented herein before determining the allowability of the newly presented claims. (A) No exhibits were shown or discussed; (B) the new independent claim 163 was discussed; (C) the discussion of prior art was limited to *Hayes* and to a lesser extent, *Doi*; (D) other than new claim 163, no other amendments were officially presented or discussed; (E) Applicant explained the teachings of *Hayes* and *Doi* and explained, consistent with the arguments presented herein, why *Hayes*, *Doi*, and the other references of record do not anticipate or make obvious the newly-presented claims; (F) no other matters were discussed; and (G) no agreements were reached regarding the claims and the examiner indicated that Applicants should submit the present amendment for consideration.

The amendments herein and comments that follow are intended to be consistent with the discussion during the interviews.

In the event that the foregoing record is not considered complete and accurate, the examiner is respectfully requested to bring any incompleteness or inaccuracy to the attention of the undersigned.

III. Arguments in Support of Allowability of New Claims Over Cited Art

In response to the objections and rejections raised in the Office Action of April 27, 2007, and in order to expedite continued examination of the present case and, hopefully, to bring this case to final resolution, Applicant hereby presents a substantive response and arguments explaining why the newly presented claims 163-191 define over and are not obviated by the art of record

Claim 163 is directed to a method for preventing unauthorized access to a specific resource within a computer network, comprising assigning a unique, non-dynamic system identifier (SID) to each authorized computer within the network; assigning a unique user identifier (UID) to each authorized user of the network; defining policy profiles for authorized computers and for authorized users of the network, wherein each policy profile identifies rights of access to resources within the network for the authorized users and the authorized computers; upon initiation of a TCP/IP communication attempt for access to the specific resource, wherein the communication attempt is initiated by a specific authorized user logged into a specific authorized computer and wherein the communication attempt includes a synchronization packet having a SEQ and an ACK field, inserting the UID of the specific authorized user and the SID of the specific authorized computer into the SEQ and ACK fields of the synchronization packet; intercepting the synchronization packet within the computer network; extracting the UID and SID from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt; and allowing the communication attempt with the specific resource as a function of the policy profile of the specific authorized user and of the policy profile of the specific authorized computer.

The other newly-presented independent claim, claim 179, is directed to a method of monitoring a TCP/IP communication attempt within a computer network, comprising assigning a unique, non-dynamic system identifier (SID) to each authorized computer within the network; assigning a unique user identifier (UID) to each authorized user of the network; upon initiation of a TCP/IP communication attempt with a requested resource within the network by a specific authorized user logged into a specific

authorized computer, inserting the UID of the specific authorized user and the SID of the specific authorized computer into SEQ and ACK fields of a synchronization packet associated with the TCP/IP communication attempt; intercepting the synchronization packet within the computer network and prior to access of the requested resource; extracting the UID and SID from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt; allowing the communication attempt with the requested resource to proceed; and logging the communication attempt in a database to maintain a record of the specific authorized user and the specific authorized computer initiating the communication attempt.

Newly presented independent claims Claims 163 and 179 clearly define the nature and scope of the present invention and in a manner that patentably distinguishes the present invention from the teachings of Hayes, Doi, Cunningham, and the other references cited by the Patent Office alone or in combination with any known or cited art.

Specifically, *Hayes* is directed to a system and method for "concealing a network device." [Hayes, Title and Abstract]. Authorized machines within Hayes' system are provided with an authorization key. [Hayes, paras. 0011 and 0012]. Such authorization key is then embedded into the SEQ and ACK fields of a TCP/IP communication. *Id.* If the validation key is contained in the SEQ and ACK fields of the synchronization packet of the communication, the network allows the communication to proceed. [Hayes, para. 8] If the validation key is not contained therein, the communication is merely dropped, which enables the resource the machine is trying to access to remain concealed. *Id.*

The validation key of Hayes, however, does not provide any information about the user or computer initiating the communication since "the key exchange mechanism is outside the scope of this invention." [Hayes, para. 0011]. The validation key is a 64-bit number that is provided to authorized machines of the network. *Id.* The validation key of Hayes could either be a one-time use random number or a commonly shared secret that could be provided to all authorized machines within the network. Bottom line, if you have the validation key, then you are granted access. Hayes, of course, explains that other information, such as date and time of the communication and IP address of the

requestor, and other information that can be carried on a TCP/IP connection request can be used, in conjunction with the verification key, for allowing the communication to proceed. However, such other information does not include user identifiers or system identifiers that are unique and assigned to authorized users and authorized computer devices within the system.

Importantly, Hayes does not teach, discuss, suggest, contemplate, or require insertion or extraction of a unique, non-dynamic system identifier (SID) or a unique user identifier (UID) associated with the communication attempt. The reason for this is because Hayes is focused on concealing requested resources on a network from unauthorized machines. In contrast, the present invention is focused on identifying the specific user and the specific computing device attempting to make a communication. Use of a unique and non-dynamic system identifier (in contrast with inherently unreliable and dynamically changing IP address) and use of a unique user identifier enables the present invention to make very specific, detailed, and actionable information upon which to make access decisions. The policy profiles, which hinge upon and which rely upon specific users and specific devices from which the communication attempt is initiated, allow the system to make such actionable decisions. Hayes is not directed to this type of use or purpose and has no need for this specific detail and information; thus, there is no need or reason for Hayes to include or explain how and why such information would be needed or useful. Hayes does indicate that additional "known" information that is available from conventional TCP/IP communications can be used, in conjunction with the validation key, for making the decision as to whether the connection is established or dropped, which conceals the requested resource from unauthorized users. However, the present invention does not use or require this additional conventional information that is available in a conventional TCP/IP communication. The present application uses the newly-defined and created SID and UID precisely because of the unreliability of the conventional information in a TCP/IP communication and precisely because it is easy to hack or fake such information that Hayes relies upon.

Hayes also does not teach, discuss, suggest, contemplate, or require allowing the communication attempt with the requested resource to proceed; and logging the

communication attempt in a database to maintain a record of the specific authorized user and the specific authorized computer initiating the communication attempt. The purpose of Hayes is to block unauthorized communication attempts or communications by unauthorized machones. Claim 179, in contrast, allows the communication attempt to proceed. Hayes also does not enable one to log and record the specific authorized user and the specific authorized computer initiating the communication attempt because the verification key of Hayes does not provide that level of detail or information.

Hayes, thus, does not anticipate the present invention and Applicants respectfully submit that it is inappropriate merely to combine Hayes with any of the many known patents and systems in existence that use conventional user IDs, device IDs, or passwords for authentication purposes. To their knowledge, Applicants are the first to conceive and invent a practical, effective, and efficient manner of using and embedding unique user identifiers and device identifiers within conventional fields within a TCP/IP synchronization packet in such a way that the information could be used, extracted, acted upon, and all without interfering with a standard TCP/IP communication protocol. The present invention hinges upon use of this critical information, which enables a network to identify the specific user and specific device initiating an electronic communication. In addition, the present invention defines policy profiles for specific users and specific computing devices, which are tied to the user and device identifiers, that enables "smart" decisions about the communication attempt to be made.

Doi, which the Patent Office has cited and relied upon as one example of the use of identifiers (here ID-information) for tracking purpose, does not alone or in combination with Hayes anticipate or obviate the newly present claims. Specifically, Doi teaches a manner of tagging information, data, or files to prevent illegal copying or to track copies that have been made. Specifically, such ID-information include user identifiers, credit card information, device manufacturer, terminal name, and serial number, and time and date in which the underlying information, data, or file is downloaded by the user. As explained in conjunction with Figs. 5-21 of Doi, this ID-information is actually embedded within the data or file in such a manner that it does not interfere with reading or access to the file, but in a manner that the system can identify

for tracking illegal or unauthorized copies of such files. This is especially useful for limiting and tracking unauthorized copies of video, movies, music, and data files that are sold on the Internet. The Patent Office has, mistakenly, relied upon one statement in Doi, associated with Fig. 4, that explains that ID-information can be "added as part of the header" of the packet used to store the underlying data. [Col. 4, lines 1-7]. The data packet referenced by Doi, however, is not and should not be confused with a communication or IP packet as used in TCP/IP communications and which are used to transmit pieces of data, bits at a time, from one device to another. The data packet of Doi is more similar to a data file in which the header is merely part of the properties associated with the underlying file. Doi merely describes this type of tagging of a data file as one alternative, which is less desirable and hidden that the process of embedding the ID-information within the data itself, which Doi focuses on.

Doi does not disclose, teach, or suggest a method for preventing unauthorized access to a specific resource within a computer network, does not define policy profiles for authorized computers and for authorized users of the network, wherein each policy profile identifies rights of access to resources within the network for the authorized users and the authorized computers, is not directed to use of a TCP/IP communication attempt for access to the specific resource, wherein the communication attempt is initiated by a specific authorized user logged into a specific authorized computer and wherein the communication attempt includes a synchronization packet having a SEQ and an ACK field, does not teach, suggest, or disclose the insertion of user and system identifiers into the SEQ and ACK fields of the synchronization packet; intercepting the synchronization packet within the computer network; extracting the identifiers from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt; and allowing the communication attempt with the specific resource as a function of the policy profile of the specific authorized user and of the policy profile of the specific authorized computer.

Doi also does not disclose, teach, or suggest a method of monitoring a TCP/IP communication attempt within a computer network; upon initiation of a TCP/IP communication attempt with a requested resource within the network by a specific

authorized user logged into a specific authorized computer, inserting a user identifier (UID) of the specific authorized user and a unique, non-dynamic system identifier (SID) of the specific authorized computer into SEQ and ACK fields of a synchronization packet associated with the TCP/IP communication attempt; intercepting the synchronization packet within the computer network and prior to access of the requested resource; extracting the UID and SID from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt; allowing the communication attempt with the requested resource to proceed; and logging the communication attempt in a database to maintain a record of the specific authorized user and the specific authorized computer initiating the communication attempt.

The Patent Office also continues to rely upon Cunningham; however, Cunningham does not anticipate or obviate alone or conjunction with Hayes, Doi or any other known or cited reference, the newly present claims.

Specifically, Cunningham discloses and teaches a method and system for monitoring and controlling access to a network by *non-intrusively* monitoring network traffic. [Cunningham, Col. 6, lines 46-48 (emphasis added)]. Cunningham explains that network access decisions can be made by intercepting and examining low level information that is contained in a conventional data packet (not a TCP/IP synchronization packet), such as "(1) the Ethernet addresses of the source and destination nodes; (2) the IP addresses of the source and destination nodes; and (3) the IP port number of the destination node." *Id.* at Col. 7, lines 7-9.

Cunningham also explains that more sophisticated network access decisions can be made by examining "higher level" information obtained from the data fields of such packets. Specifically, "the packets that are specific to a particular node-to-node transmission can be *collected* and *assembled*....The workstation then has the capability of *piecing together the fragments of a multi-packet signal*." *Id.* at Col. 7, lines 21-26 (emphasis added). Thus, "[h]igher level decisions can be formed *only* after a connection has been established and the *actual content* has begun to flow over that connection." *Id.* at Col. 8, lines 3-5 (emphasis added). Thus, Cunningham teaches how to make intelligent

use of information that is already included in all conventional data packets, such as Ethernet addresses, IP addresses, and IP ports. Alternatively, Cunningham teaches how to make high level or more sophisticated decisions about network access by collecting and assembling a plurality of data packets in a communication stream and piecing together the user or application data that can only be obtained by assembling and analyzing a plurality of packets. In either case, Cunningham merely takes advantage of the standard information obtained from conventional data packets.

Cunningham does not teach, disclose, or suggest a method for preventing unauthorized access to a specific resource within a computer network, comprising assigning a unique, non-dynamic system identifier (SID) to each authorized computer within the network; assigning a unique user identifier (UID) to each authorized user of the network; defining policy profiles for authorized computers and for authorized users of the network, wherein each policy profile identifies rights of access to resources within the network for the authorized users and the authorized computers; upon initiation of a TCP/IP communication attempt for access to the specific resource, wherein the communication attempt is initiated by a specific authorized user logged into a specific authorized computer and wherein the communication attempt includes a synchronization packet having a SEQ and an ACK field, inserting the UID of the specific authorized user and the SID of the specific authorized computer into the SEQ and ACK fields of the synchronization packet; intercepting the synchronization packet within the computer network; extracting the UID and SID from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt; and allowing the communication attempt with the specific resource as a function of the policy profile of the specific authorized user and of the policy profile of the specific authorized computer.

Cunningham also does not teach, suggest, or disclose a method of monitoring a TCP/IP communication attempt within a computer network, comprising assigning a unique, non-dynamic system identifier (SID) to each authorized computer within the network; assigning a unique user identifier (UID) to each authorized user of the network; upon initiation of a TCP/IP communication attempt with a requested resource within the

network by a specific authorized user logged into a specific authorized computer, inserting the UID of the specific authorized user and the SID of the specific authorized computer into SEQ and ACK fields of a synchronization packet associated with the TCP/IP communication attempt; intercepting the synchronization packet within the computer network and prior to access of the requested resource; extracting the UID and SID from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt; allowing the communication attempt with the requested resource to proceed; and logging the communication attempt in a database to maintain a record of the specific authorized user and the specific authorized computer initiating the communication attempt.

For the above reasons, newly presented independent claims 163 and 179 are allowable over the references of record. Similarly, since dependent claims 164-178 and 180-191 merely provide additional details and limitations to independent claims 163 and 179, respectively, such dependent claims should be allowable for the same reasons as independent claims 163 and 179.

Thus, for at least the above reasons, independent claims 163 and 179 define over the references cited by the Patent Office to date, including Hayes, Doi, and Cunningham, whether considered alone or in combination with any of the other references known or cited. For these reasons, newly presented independent claims 163 and 179, and all of their dependent claims, should stand in condition for allowance.

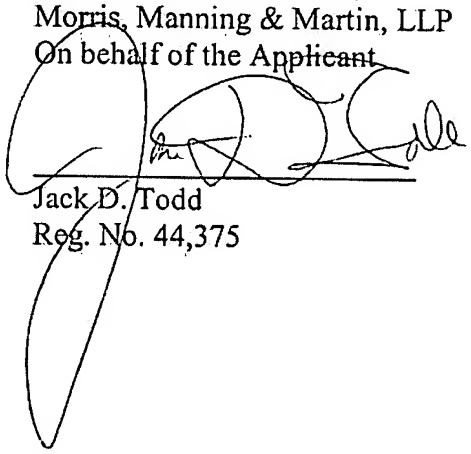
CONCLUSION

It is respectfully submitted that newly presented claims 163-191 are not anticipated by or rendered obvious by any of the art cited by the Patent Office to date, including Hayes, Doi, and Cunningham, whether considered alone or in combination with any of the other references cited. For these reasons, Applicant respectfully submits that newly presented claims 163-191 define over the references known or cited and, thus, stand in condition for allowance, which action is earnestly solicited.

Since Applicant originally paid for 7 independent and 117 total claims, it is respectfully submitted that no additional claim fees are due with this response, which has

been reduced to 2 independent claims and 29 total claims. Applicants submit the present Response and Amendment with a Petition and fee for 2 month extension of time. However, if our assessment of fees due is in error, please charge any fees that might be due or credit any overpayment to our Deposit Account No. 50-3537.

Respectfully submitted by
Morris, Manning & Martin, LLP
On behalf of the Applicant



September 27, 2007

Jack D. Todd
Reg. No. 44,375

Morris, Manning and Martin, LLP
1600 Atlanta Financial Center
3343 Peachtree Road, N.E.
Atlanta Georgia 30326
404-504-7674 Direct
404-233-7000 Main